REMARKS

We have amended the claims to address the informalities identified by the examiner. Among the amendments we have made, we have changed "encrypted container" to read "personal security device." We have also canceled claim 56. Upon entering these amendments, claims 1, 3-5, 10-11, 13-14, 17-18, 52-55, and 57-90 will be pending in the application.

We conducted a telephone interview with the examiner on January 10, 2006, during which we discussed the comments he made in the Advisory Action and sought further clarification of his rejections.

The examiner rejected claims 1, 11, 52, and 53 under 35 U.S.C. §103(a) as being unpatentable over Holloway (U.S. 6,424,718) in view of Linehan (U.S. 5,495,533). As previously noted, the examiner admitted that Holloway fails to teach:

> (c) at an authentication server, receiving authentication information from the client; and
> (d) responsive to said authentication information, sending from a key server to the client decryption information for said personal security device.

To supply that which is missing, the examiner relied on Linehan as supposedly teaching these elements. The examiner argued that it would be obvious to incorporate them into Holloway because:

> ...disadvantages of manual key management (such as entering Holloway's owner's pass phrase PPu) include the awkward and time-consuming requirements for end-users to enter encryption keys, the possibility that users may forget keys, the inability to access encrypted files when the individual who knows the keys is unavailable.

The examiner's argument presents three specific reasons why a person skilled in the art would be motivated to combine the features of Linehan with Holloway. But none of these reasons stand up under closer scrutiny.

8

First, the examiner argues that the Linehan system would reduce the burdens on the user that exist in the Holloway system. But that is not true. The burdens would be no less, yet the complexity of the resulting system would be much greater.

The examiner points out that the Holloway system requires that the user enter a pass phrase PPu in order to authenticate. The examiner characterizes this step as "awkward and time-consuming," and that presumably Linehan would do away with the burden. We note, however, that the Linehan system **also requires the user to enter a pass phrase in order to authenticate**. Linehan discloses that "[t]he 'foundation' for access to files is the Kerberos or KryptoKnight authentication of individual users" (col. 11, lines 7-9). According to Linehan, a user authenticates to Kerberos with a password:

> A network authentication mechanism, such as Kerberos (reference 8), keeps the
> password file on a authentication server 20 as shown in FIG. 3. A special
> protocol is used to validate a userid and password entered on a user computer
> 22 against the password file on the authentication server 20. (col. 3 lines 10-
> 14).

In other words, the user must enter a password to authenticate in the Linehan system. So, including the personal key server and authentication server of Linehan in the system of Holloway, though it would make the Holloway system more complex, would not make it less awkward or less time-consuming for a user to enter a password.

The other reasons the examiner provides as a motivation to combine the features of Linehan with Holloway, namely "the possibility that users may forget keys," and "the inability to access encrypted files when the individual who knows the keys is unavailable," are completely contrary to the stated goals of the Holloway system. Holloway states:

> The present invention is directed to the problem of providing a secure method of enabling
> messages to be processed using public key processing on behalf of an authorized user in
> such a manner that it can be shown that **only the authorized user** could have authorized
> the processing of a particular message (col. 3, lines 18-23, emphasis added).

Holloway is very concerned with keeping the key secure, and accessible only by the user. Holloway discloses accomplishing this goal by, among other things, encrypting the key under user pass phrase PPu (col. 8, lines 20-22). Anyone without pass phrase PPu cannot decrypt the key. Thus, Holloway actually teaches away from enabling parties other than the user from being able to access the key.

The examiner suggests that combining the system of Linehan with Holloway would prevent the loss of a key if the user forgets his password. But Holloway replaces the key if the password changes, i.e., if the user forgets it and selects another:

> The private key record may have changed because, for example, the pass phrase and therefore the encryption key has changed, or because a new signature private and public key pair are generated. Both cases are treated as if both the pass phrase and the private/public key pair have changed…At server system 130, the public and private key records are replaced (col. 10, lines 13-22).

An objective of Holloway's system is to prevent others from ever being able to access the key. To accomplish this objective, among other things, his system generates new keys and encrypts them under new passwords as necessary.

The examiner also suggests that combining the system of Linehan with Holloway would allow someone to access a key in the absence of the user. But, as noted above, Holloway's system is explicitly designed to **prevent anyone but the user** from accessing the key. Indeed, Holloway discloses deleting the key to prevent its access by others:

> [I]f the signer's private key is compromised, a different user might use it to process messages. In this circumstance, a means is required to revoke the secret key so the unauthorized user can no longer use it (col. 2, lines 29-32).

> It will be appreciated that, as server 130 holds the private key, albeit enciphered, server system 130 can deactivate the key by simply erasing it. It is then no longer available for signing (col. 10, lines 28-31).
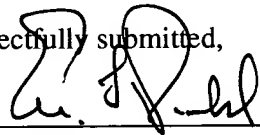
Including Linehan's personal key server and authentication server in order to be able to access a key in the absence of the user, as the examiner proposes, is fundamentally counter to a main purpose of Holloway. Holloway's system is designed to **prevent** others from accessing the user's key. Thus, Holloway teaches away from making the changes proposed by the examiner.

For at least these reasons, we request the examiner withdraw his rejection of the claims and allow the pending application to issue.

A petition for a three-month extension of time accompanies this Response, and the commissioner is hereby authorized to charge Deposit Account No. 08-0219 the fee of $1,020 to cover the cost of this extension. No other fees are believed to be due at this time. However, please charge any fees, or credit any overpayment, to Deposit Account No. 08-0219.

Dated: January 17, 2006　　　　　　　　　　Respectfully submitted,

By_____
Eric L. Prahl
　　Registration No.: 32,590
WILMER CUTLER PICKERING HALE AND
　　DORR LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000
Attorney for Applicant

11